ExtremeXOS Operating System, Version 12.4

ExtremeXOS® Operating System—a highly available, secure, open and extensible foundation for high-performance Ethernet-based converged networks.

High Availability Architecture

- Reduce network downtime using hitless failover and module-level software upgrade
- Prevent system corruption using memory protection for processes
- Avoid system reboots using self-healing process recovery

Extensibility

- Integrate best-of-breed applications to your network with an open, yet secure XML-based Application Programming Interface (API)
- Integrate Extreme Networks and third-party developed software applications using open standards-based POSIX interfaces
- Scripting-based device management for incremental configuration deployment and ease of management

Integrated Security

- Guard access to the network through authentication, Network Login/802.1x, host integrity checking, and Identity Management
- Harden the network infrastructure with Denial of Service (DoS) protection and IP Security against man-in-the-middle and DoS attacks
- Secure management using authentication and encryption

The ExtremeXOS OS provides the reliable transport needed for converged network services using a variety of resiliency protocols.

Extreme Networks® has revolutionized the industry by creating the ExtremeXOS modular Operating System (OS)—a highly available and extensible foundation for high-performance networks. ExtremeXOS raises the bar for availability, critical for offering carrier-grade voice and video services over IP and for supporting mission-critical business applications.

Built-in security capabilities provide network access control integrated with end-point integrity checking, identity management, and protection for the network control and management planes.

With an ExtremeXOS OS you can extend the capabilities of your network by integrating specialized application appliances such as security devices into the network, providing insight and control at the network, application and user level.

Architectural Highlights

- Memory Protection for Processes
- Self-Healing Process Recovery via Process Restart or Hitless Failover
- Dynamic Loading of New Functionality
- Scriptable CLI for Automation and Event Triggered Actions
- XML Open APIs for Integrating Third-Party Applications
- Dual-stack IPv4 and IPv6 Support

High Availability

Continuous network uptime and predictable service quality is vital for mission-critical applications such as virtualized Data Centers, converged Enterprise campuses, Carrier Ethernet deployments and many others. The high availability of the ExtremeXOS OS creates a resilient infrastructure capable of maximum network integrity for mission-critical applications.

Modular Operating System

True preemptive scheduling and memory protection allow each of the many applications—such as Open Shortest Path First (OSPF) and Spanning Tree Protocol (STP)—to run as separate OS processes that are protected from each other. This provides increased system integrity and inherently protects against DoS attacks.

The ExtremeXOS OS dramatically increases network availability using process monitoring and restart. Each independent OS process is monitored in real time. If a process becomes unresponsive or stops running, it may be possible to automatically restart, or other automatic corrective actions such as hitless failover to a redundant management module or standby stack master can be taken.

The modular design of the ExtremeXOS OS allows the upgrading of certain individual software modules, should this be necessary, leading to higher availability in the network (see Figure 1). This includes security stacks such as SSH and SSL as well as the Converged Network Analyzer VoIP SLA monitoring agent.

Hitless Failover and Graceful Restart

With dual management modules on BlackDiamond® chassis systems and advanced stacking support with Summit® fixed-configuration switches, the ExtremeXOS OS is capable of preserving the state of resiliency and security protocols such as STP, EAPS and Network Login, thus allowing hitless failover between management modules/redundant masters in case a module or master fails.

Graceful restart is a way for OSPF-2, BGP-4 and IS-IS protocols to restart without disrupting traffic forwarding. Without graceful restart, adjacent routers will assume that information previously received from the restarting router is stale and won't be used to forward traffic to that router. If the peer routers support the graceful restart extensions, then the router can restart the routing protocol and continue to forward traffic correctly.

Powered by ExtremeXOS, the BlackDiamond chassis systems separate the forwarding function from the control function so that traffic can still be forwarded independently of the state of the routing protocol function. Routes learned remain in the routing table and packets continue to be forwarded.

If the network topology is not changing, the static routing table remains correct. In most cases, networks can remain stable (i.e. would not re-converge) during the time for restarting OSPF, BGP or IS-IS. Should route updates still exist, graceful restart incrementally performs these updates after the restart.

CPU Denial of Service Protection

A DoS attack is an explicit attempt by an attacker to degrade or disable a switch by overwhelming the switch's system resources. CPU DoS protection prevents attacks from crippling the switch. Enhanced CPU DoS protection capability from Extreme Networks can detect, analyze and respond to threats directed at the switch CPU. The technique uses counters to categorize and monitor traffic flow into the switch's CPU. If the traffic to the CPU exceeds a certain threshold, the switch will examine that traffic, determine if a threat exists and activate a dynamic ACL to prevent packets of the same type from disrupting switch operations.

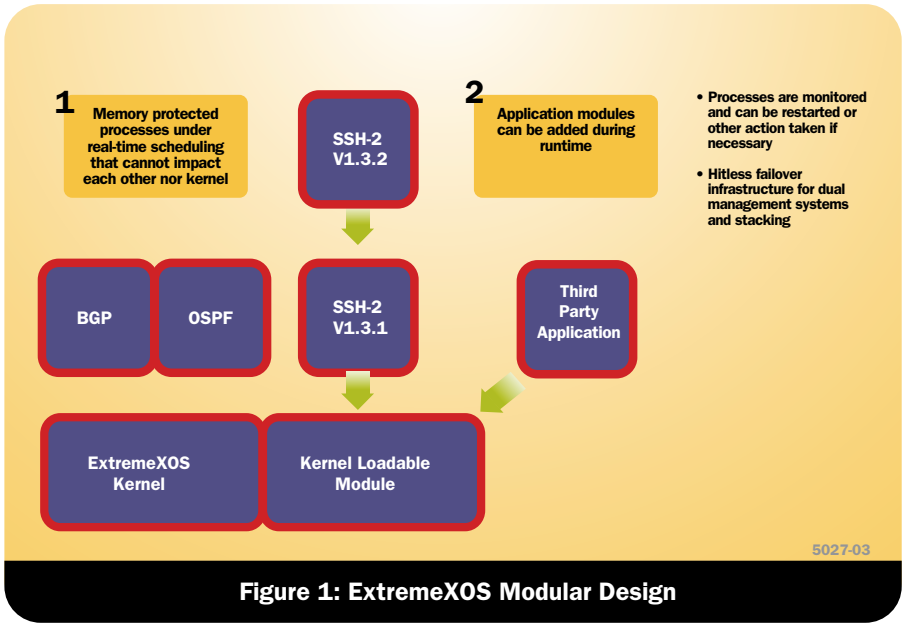

1
Memory protected processes under real-time scheduling that cannot impact each other nor kernel
SSH-2 V1.3.2
2
Application modules can be added during runtime
• Processes are monitored and can be restarted or other action taken if necessary
• Hitless failover infrastructure for dual management systems and stacking
BGP
OSPF
SSH-2 V1.3.1
Third Party Application
ExtremeXOS Kernel
Kernel Loadable Module
5027-03

Figure 1: ExtremeXOS Modular Design

© 2010 Extreme Networks, Inc. All rights reserved.

Extensibility

Dynamically loadable software application modules, CLI scripting and external XML APIs make the ExtremeXOS OS extensible, allowing integration with best-of-breed applications and devices, providing endless possibilities for further expanding the network's capabilities. Examples include VoIP monitoring and advanced network security.

Dynamic Module Loading

The ExtremeXOS OS provides an infrastructure to dynamically load, start and gracefully stop new applications. ExtremeXOS embraces POSIX-compliant interfaces that ease the integration of new applications. ExtremeXOS uses this infrastructure to dynamically load Extreme Networks developed functionality such as SSH/SCP/SSL that is export-controlled, avoiding the requirement for new operating system image installs to gain this functionality. The same infrastructure is also used to integrate third-party developed applications. An example is the VoIP application layer monitoring agent developed by Avaya to simulate and closely monitor VoIP connection behavior in a network.

Scripting

ExtremeXOS provides a CLI scripting infrastructure. Scripting can be used to add incremental configuration to the network infrastructure, such as a list of VLANs to be configured. This capability eases the roll-out of networks and reduces configuration errors. Scripting capabilities, such as system- and user-defined environment variables, and constructs, such as if/then and loops, allow automating regular management tasks in scripts and deploying configurations such as QoS, rate limiting and ACLs, for example, to multiple ports. Scripts can access CLI output, and a rich set of Tcl functions provides a utility library of string manipulation, search or mathematical functions. By leveraging scripting for switch configuration, rolling out a new switch can be reduced to minutes and just a few commands for switch-specific settings. Scripting is also used in the ExtremeXOS Universal Port framework to define trigger event actions.

XML Application Programming Interfaces

Extreme Networks has pioneered an innovative approach to communications on the network control plane. Using XML APIs—concepts originally developed in the emerging field of Web services—the ExtremeXOS OS can provide select third parties a secure, simple mechanism to access processes within the switch (see Figure 2). For example, a security appliance can utilize ExtremeXOS to limit access, control bandwidth or redirect traffic from a client that is attempting to connect to the network. XML also provides a scalable and reliable transport for device configuration and statistics, for example OSS and service provisioning systems in Carrier Ethernet deployments.

This XML infrastructure embraces the concept of open yet secure communications to allow business applications to easily interact with the network for security policy enforcement, regulatory compliance and performance management, and higher security.

The XML infrastructure is also used by ExtremeXOS ScreenPlay™ Web-based management interface.

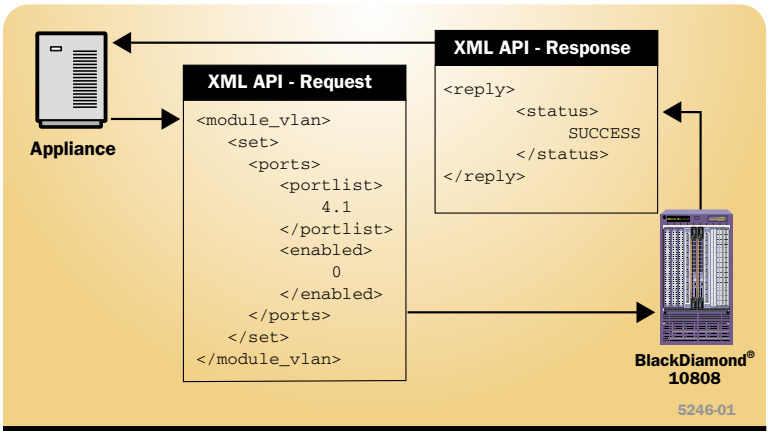


Figure 2: XML-based Communications

```
X450e-24p.2 # create upm profile detect-avaya
Start typing the profile and end with a . as the
  first and the only character on a line.
Use - edit upm profile <name> - for block
  mode capability
create log entry Starting_Script_DETECT-AVAYA
set var callServer 192.168.10.204
set var fileServer 192.168.10.194
set var voiceVlan Voice
set var CleanupProfile CleanPort
set var sendTraps false
create log entry Starting_DETECT-AVAYA
  _Port_$EVENT.USER_PORT
```

5245-01

Figure 3: Example of CLI Scripting for Universal Port

© 2010 Extreme Networks, Inc. All rights reserved.

Ease of Management

Standards-based discovery and traffic flow monitoring provide full visibility into network inventory and traffic. ExtremeXOS Universal Port dramatically simplifies rollout of VoIP via auto-configuration of edge ports and phones.

Link Layer Discovery Protocol (LLDP, IEEE 802.1ab)

Today's networks must incorporate best-of-breed solutions at every layer of the network, regardless of which vendor you choose, allowing you to build a best-of-breed converged network.

The ExtremeXOS OS support of IEEE 802.1ab standards-based discovery protocol provides vendor-independent device discovery as well as tight integration with VoIP infrastructure and phones, including E911 ECS location, inventory information and fine-grained PoE budgeting and configuration of information such as VLANs and QoS tagging.

LLDP not only simplifies deployment and locating of access devices, but it can also be used as a troubleshooting and firmware management tool.

LLDP is an extensible standard, providing a framework for industry consortiums to define application-specific extensions without causing compatibility issues. The ANSI/TIA-1057 LLDP-Media Endpoint Discovery (LLDP-MED) standard defines extensions specifically for VoIP. These extensions provide VoIP-specific information as well as allow transmission of configuration and location information to VoIP phones.

- Network Policy (which VLAN tag, .1p, DSCP, … that the phone should use)
- ECS Location ID (for E911 – coordinates for street/building/floor address), compliant with NENA and TIA-TSB-146 directions. The switch advertises a configurable physical location information to the phone
- Extended Power-via-MDI (finer grain PoE budget management)
- Inventory information such as firmware version, serial number, etc.

LLDP is tightly integrated with the IEEE 802.1x authentication at edge ports. As endpoint devices are first authenticated, the LLDP-provided information is trustable and can be used for automated configuration, protecting the network from attacks against automated configuration mechanisms.

sFlow

ExtremeXOS OS's sFlow® standards-based data monitoring support provides Layer 2 – 7 visibility into the network, including statistics on which applications are running over your network, biggest talkers, etc.

With the ever-increasing reliance on network services for business-critical applications, the smallest change in network usage can impact the performance and reliability of a network. This has a direct impact on the ability of a company to conduct key business functions and on the cost of maintaining network services. Therefore, it is important to monitor the network traffic in order to keep the network operating reliably and at the right performance level.

sFlow is a sampling technology that meets the key requirements for a network traffic monitoring solution: sFlow provides a network-wide view of usage and active routes. It is a scalable technique for measuring network traffic, collecting, storing, and analyzing traffic data. This enables tens of thousands of interfaces to be monitored from a single location.

sFlow is scalable, thereby enabling it to monitor links of speeds up to 10 Gigabits per Second (Gbps) and beyond without impacting the performance even of core Internet routers and switches, and without adding significant network load.

Universal Port

The unique ExtremeXOS OS Universal Port infrastructure is a powerful framework of event-driven activation of CLI scripts. While Universal Port can leverage any system event log message as an event trigger, the most popular use cases are time/user/location-based dynamic security policies as well as VoIP auto-configuration. For these applications, Universal Port uses standards authentication (Network Login/802.1x) and discovery protocols (LLDP + LLDP-MED) as trigger events. Actions in the form of fully configurable CLI scripts can be tied to events on a per-port basis. As such, dynamic security policies, including fine-grained access control via ACLs, can follow a user independently of where he logs into the network. VoIP phones and the connecting switch edge port can be auto-configured for the voice VLAN and QoS. The switch can receive the exact, fine-grained power budget requirements from the phones and provision it accordingly. The phone can receive the E911 ECS location from the switch as well as the call server address in order to receive additional configuration. Deploying VoIP endpoints is as easy as opening the package, programming the extension and plugging into the network. The following diagram explains the mechanism. Please note that steps 1 and 2 are only done once, using scripting, and then rolled out to all voice-capable ports. Steps 3 to 5 are the resulting automatic runtime events.

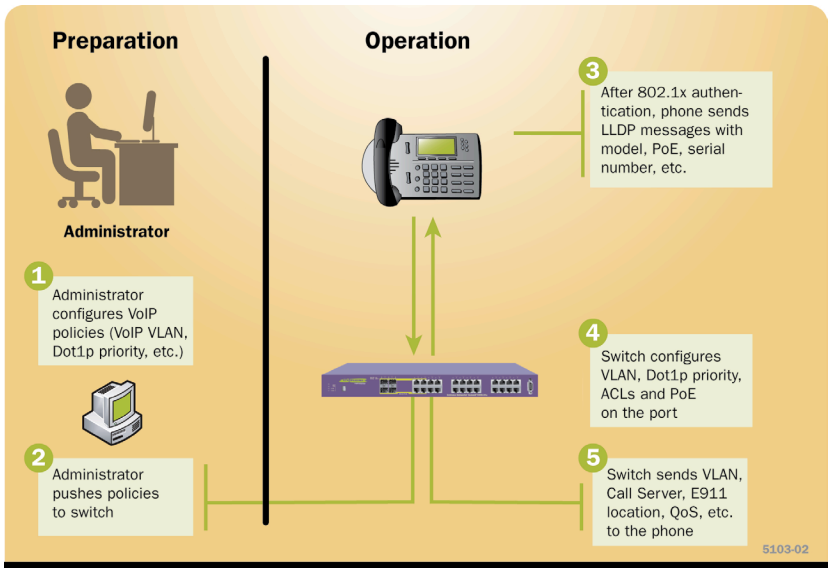

Preparation
Operation
Administrator
1
Administrator configures VoIP policies (VoIP VLAN, Dot1p priority, etc.)
2
Administrator pushes policies to switch
3
After 802.1x authentication, phone sends LLDP messages with model, PoE, serial number, etc.
4
Switch configures VLAN, Dot1p priority, ACLs and PoE on the port
5
Switch sends VLAN, Call Server, E911 location, QoS, etc. to the phone
5103-02

Figure 4: VoIP Auto Configuration with ExtremeXOS Universal Port

© 2010 Extreme Networks, Inc. All rights reserved.

Integrated Security

Security of the entire network infrastructure is protected with the ExtremeXOS OS. Protection at the edge is provided with user authentication, host integrity checking and dynamic user/time/location based security policies. Management traffic is secured through authentication and encryption.

Network Login

Extreme Networks pioneered network access security even before dedicated standards' efforts were in place. Its open, standards-based approach allows network access control on all edge ports of a network. Access control works with or without dedicated authentication support on client devices, such as VoIP phones and printers.

Network Login enforces authentication before granting access to the network. All packets sent by a client on the port will not get beyond the port to the rest of the network until authentication using RADIUS servers occurs. In many cases, the RADIUS server will interact with central data repositories for user authentication such as Active Directory or an LDAP directory without putting the burden of the LDAP protocol into the network infrastructure. As a fallback for mission-critical devices, debugging and simplicity, an authentication database local to the switch can be used as well.

ExtremeXOS Network Login supports multiple supplicants on the same switch edge port, even in separate VLANs. For example, a VoIP phone can be authenticated into the voice VLAN, and a PC connected to the data port of the phone can be authenticated into a user-specific VLAN.

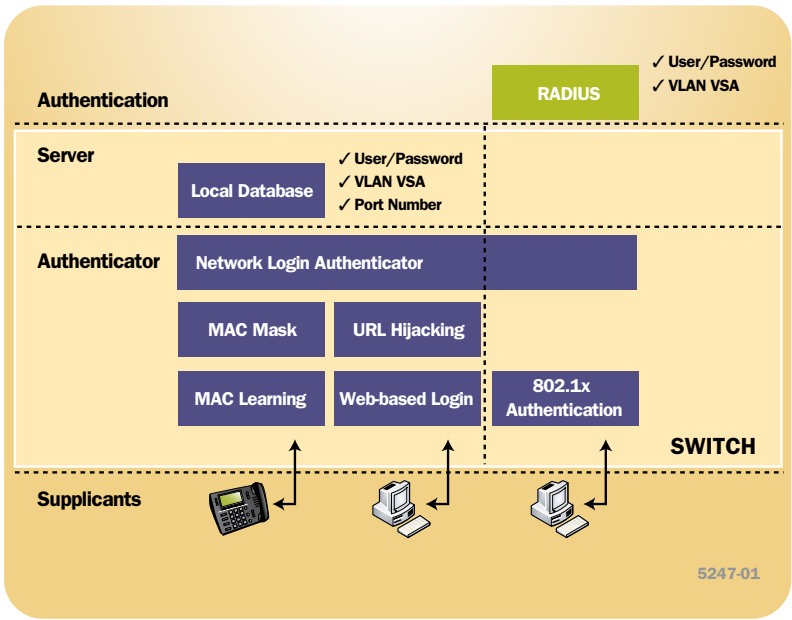
Network Login supports three methods: 802.1x, Web-based and MAC-based. All methods can be enabled individually or together to provide smooth implementation of a secured network.

802.1x is a standards-based protocol that requires a special client be installed on the system accessing the network. Over time, 802.1x will be a standard component in PC operating systems as well as networked devices such as VoIP phones. 802.1x is designed as a secure protocol, and uses a number of different secure authentication techniques. ExtremeXOS supports a variety of these techniques, including MD5, PEAP, TLS and TTLS, supporting password- as well as certificate-based authentication.

The Web-based method does not require any specific client-side software (a challenge for 802.1x). Instead the Web-based method uses standard built-in technologies on clients (DHCP and a Web browser), and therefore is an easy-to-deploy security mechanism for all client devices that support these technologies. When an unauthenticated machine's Web browser first requests traffic from any HTTP server on the network, Extreme Networks switches with Web-based Network Login enabled will redirect this traffic to the Network Login welcome page. The login welcome page is fully customizable to allow posting a custom page content and graphics, for example guest login information for Internet access via a dedicated guest VLAN and custom logos.

The Web-based method is also an excellent way to deploy 802.1x client software and certificates in a secure fashion on any port without having to open up the network. Rather than installing an 802.1x client software before turning on Network Login, users can log into the network via the Web-based method, be redirected to an IT server to receive instructions how to download and install an 802.1x client and potentially additional software. This strategy dramatically reduces the costs and complexity of a user authentication rollout in your network.

The MAC-based method is targeted for networked devices that do not support any manual authentication methods, such as older VoIP phones or printers, and hence allows the enforcement of authentication on all edge ports in a network.



© 2010 Extreme Networks, Inc. All rights reserved.

Integrated Security

Integrated Security

Dynamic security policies can be deployed via RADIUS Vendor Specific Attributes (VSAs). As an example, the VLAN for a given user or device can be dynamically assigned. Network Login optionally will even dynamically create the VLAN if it does not exist on the edge switch, dramatically reducing the burden of managing VLANs. In Extreme Networks implementation, leveraging the fully configurable ExtremeXOS Universal Port infrastructure, dynamic security policies go far beyond just VLAN assignments (see Figure 6).

Dynamic policies may also include rate limiting, QoS and dynamic ACLs. These are applied immediately during the authentication process, without dependency on external second-step policy managers. Instead, one central repository (RADIUS or LDAP/Active Directory) and a single-step approach are provided. Dynamic security policies are activated and deactivated based on authentication and hosts connecting or disconnecting from the network. As the actual implementation of the policy can be changed from port to port, the framework allows for location-based policies. Integration with a timer event provides time based policies, such as disabling wireless access after business hours.

MAC Security

MAC Security allows the lockdown of a port to a given MAC address and to limit the number of MAC addresses on a port. This can be used to dedicate ports to specific hosts or devices such as VoIP phones or printers and avoid abuse of the port—an interesting capability specifically in environments such as hotels. In addition, an aging timer can be configured for the MAC lockdown, protecting the network from the effects of attacks using (often rapidly) changing MAC addresses.

IP Security

ExtremeXOS IP security framework protects the network infrastructure, network services such as DHCP and DNS and even host computers from spoofing and man-in-the-middle attacks. It also provides network protection from statically configured and/or spoofed IP addresses as well as building an external trusted database of MAC/IP/port bindings so that you always know where traffic from a specific address comes from for immediate defense. Specific capabilities include:

- Build a trusted network database of MAC/IP/Port bindings and know where to take action if something goes wrong
  - "DHCP Option 82", adds port + VLAN ID to DHCP requests
- Enforce DHCP, protect from static IP
  - "Disable ARP Learning", only learn via DHCP
- Protect the network from random source address threats
  - DHCP Snooping based "Source IP Lockdown" automatic ACL
- Protect network from man-in-the-middle attacks and VoIP call recording
  - "Gratuitous ARP Protection" of default gateway
- Protect network services (DHCP, DNS, ...) spoofing / rogue servers
  - "Trusted DHCP Server" ports
  - "Gratuitous ARP Protection" of DNS, ... Servers
- Protect endpoints/applications from spoofing attacks
  - "DHCP secured ARP"—ARP Validation against DHCP snooping-based internal database

Identity Management

Identity Management allows customers to track users who access their network. User identity is captured based on NetLogin authentication, LLDP discovery and Kerberos snooping. ExtremeXOS uses the information to then report on the MAC, VLAN, computer hostname, and port location of the user.

Secure Management

The ExtremeXOS OS provides secure management via SSH2/SCP2/SSL and SNMPv3, providing authentication and protection against replay attacks, as well as data privacy via encryption.

Access profiles for device management allow filters to be set on device management, accepting connections only from specified sources.

CPU DoS Protect throttles traffic directed to the switch and can automatically set an ACL for defense, thus protecting the switch from the effects of DoS attacks such as "Ping of Death" and others. This defense mechanism works for all CPU bound traffic—Layer 2, IPv4 and IPv6.

Routing protocols such as OSPF-2 and BGP4 authenticate via MD5.

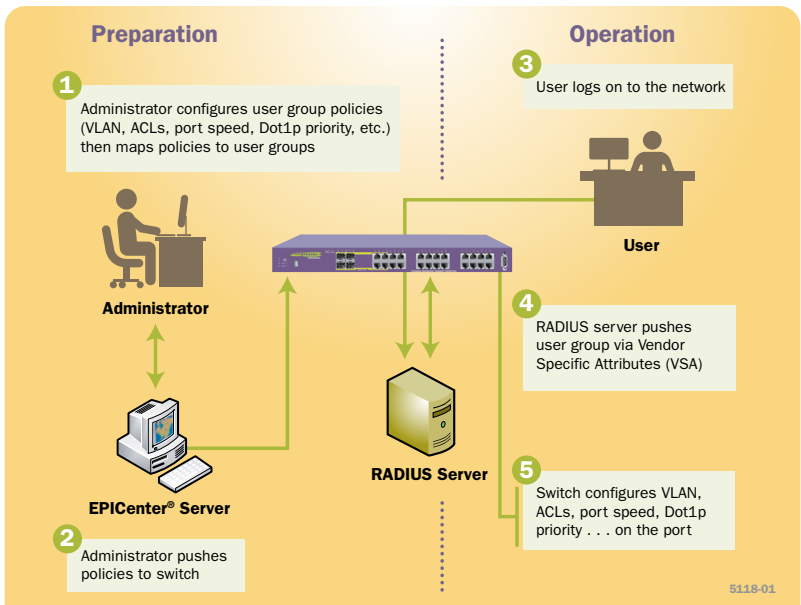


Figure 6: Universal Port Dynamic Policies

© 2010 Extreme Networks, Inc. All rights reserved.

Switching: Network Resiliency and Forwarding Control

The ExtremeXOS OS provides full flexibility for various network designs through an extensive set of Layer 2 and Layer 3 protocols, offering network wide resiliency and forwarding control that scales to large networks.

Layer 2+

For network resiliency, ExtremeXOS offers a choice between standard protocols and more advanced Layer 2+ protocols, optimized for faster resiliency, larger scaling and simpler operation.

Spanning Tree Protocol: ExtremeXOS supports IEEE 802.1D STP, 802.1w RSTP and 802.1s MSTP. In Extreme Multiple Instance STP mode, ExtremeXOS allows a port or VLAN to belong to multiple STP domains and therefore adds significant flexibility to STP network design, further increasing resiliency. The implementation is also PVST+ compatible and IEEE 802.1Q.

Ethernet Automatic Protection Switching (EAPS, RFC 3619), invented by Extreme Networks, is designed to prevent loops in a ring topology running Layer 2 traffic. Its role is similar to STP, however it is able to rapidly converge when a link breaks, transparently to VoIP calls, independent of the number of switches in a ring. Timing will be sub 50 ms in most deployments.

Resiliency Features: the Virtual Router Redundancy Protocol (VRRP) enables a group of routers to function as a single virtual default gateway. Extreme Standby Router Protocol™ (ESRP) can be implemented at both Layers 2 and 3. ESRP tracks link connectivity, VLANs, learned routes and ping responses. ESRP can be used as an STP and VRRP substitute, providing simplicity via a single protocol for Layer 2 and Layer 3 redundancy. Multiple instances of ESRP in the same VLAN allow direct host attachment to standby switches.

Virtual Private LAN Services (VPLS, RFC 4762) is used for signaling and provisioning subscriber VLANs and vMANs over IP network core. Extreme Networks VPLS implementation operates seamlessly with EAPS, ESRP, and STP to provide a connectivity option for delivering fault-tolerant Layer 2 services over a Layer 3 network core.

To further harden the network resiliency protocols of ExtremeXOS, Extreme Link Status Monitoring (ELSM) protects the network and resiliency protocols from the effects of unidirectional links to protocols. For bandwidth scaling, link aggregation (static and dynamic via LACP) utilizes the bandwidth of multiple links. IGMP Snooping and Multicast VLAN Registration preserve network bandwidth by forwarding only to ports and to VLANs with subscribers from a single multicast VLAN. If desired, static IGMP membership allows the force-forwarding of traffic through the network for snappy subscription response and filters provide control over transmitted content. EAPS, ESRP and VRRP support multiple domains per port pair and the bandwidth of a blocked port in one domain can be used by VLANs in another domain (spatial reuse). In fact, multiple instances of ESRP in the same VLAN even allow direct dual-homed host attachment—for example server farms to standby switches—while utilizing the bandwidth of the standby switch.

IPv4

ExtremeXOS offers an equally extensive set of Layer 3 switching features all geared to increasing control and management on very large networks. The switching software implements static routes, RIP, OSPFv2, IS-IS and BGP4 for External BGP (EBGP) and Internal BGP (IBGP).

ExtremeXOS fields a rich set of IP multicast routing protocols, including PIM Dense Mode (PIM/DM), PIM Sparse Mode (PIM/ SM) and PIM Source Specific Multicast (PIM-SSM), which work hand in hand with the built-in IGMPv1/v2/v3 support. Multicast source routes can be shared between sites using MSDP and MBGP, for example, to share sources of distance learning multicast streams in a university backbone network. IGMP v2/v3 SSM mapping allows both IGMPv2 and IGMPv3 in the network, upgrading to the more powerful and secure IGMPv3 where needed.

Designed for IPv6

IPv6 offers improved network intelligence and a considerable number of new capabilities over IPv4. However, there are specific challenges whether choosing to actively participate in the transition to IPv6 or holding off to further evaluate. Extreme Networks has taken a ground-up approach to addressing these challenges by designing IPv6 intelligence into ExtremeXOS from the beginning.
Extreme Networks has built an architecture that meets the performance, flexibility and security requirements of IPv6 without compromising operational simplicity (see Figure 7).

Features include Layer 2 and Layer 3 IPv6 forwarding, routing protocols and tunnels. ExtremeXOS provides investment protection and allows a safe and smooth transition by tunneling IPv6 traffic across non-IPv6-aware parts of the network.

ExtremeXOS platforms offer wire-speed ACLs—providing defense and control over the next generation of IP, which is at least partially supported by most client and server operating systems today. Even when operating with IPv4 only, the ExtremeXOS OS will harden the network to attacks using IPv6 transport.

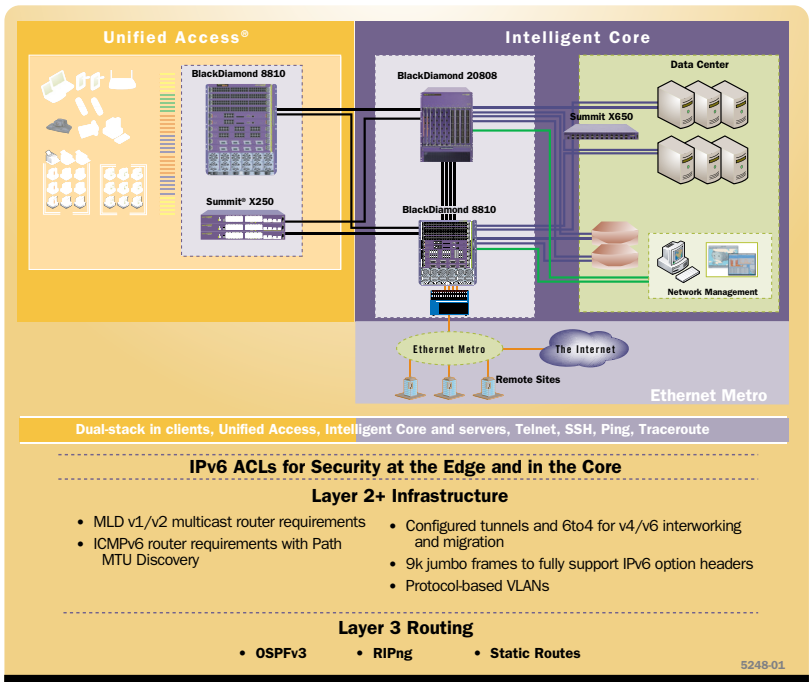


Figure 7: Edge-to-Core IPv6-Enabled Infrastructure

© 2010 Extreme Networks, Inc. All rights reserved.

Technical Specifications

ExtremeXOS 12.4 Supported Protocols

Switching

- RFC 3619 Ethernet Automatic Protection Switching (EAPS) and EAPSv2
- IEEE 802.1D – 1998 Spanning Tree Protocol (STP)
- IEEE 802.1D – 2004 Spanning Tree Protocol (STP and RSTP)
- IEEE 802.1w – 2001 Rapid Reconfiguration for STP, RSTP
- IEEE 802.1Q – 2003 (formerly IEEE 802.1s) Multiple Instances of STP, MSTP
- EMISTP, Extreme Multiple Instances of Spanning Tree Protocol
- PVST+, Per VLAN STP (802.1Q interoperable)
- Draft-ietf-bridge-rstpmib-03.txt – Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol
- Extreme Standby Router Protocol™ (ESRP)
- IEEE 802.1Q – 1998 Virtual Bridged Local Area Networks
- IEEE 802.3ad Static load sharing configuration and LACP based dynamic configuration
- Software Redundant Ports
- IEEE 802.1AB – LLDP Link Layer Discovery Protocol
- LLDP Media Endpoint Discovery (LLDP-MED), ANSI/TIA-1057, draft 08
- Extreme Discovery Protocol (EDP)
- Extreme Loop Recovery Protocol (ELRP)
- Extreme Link State Monitoring (ELSM)
- IEEE 802.1ag L2 Ping and traceroute, Connectivity Fault Management
- ITU-T Y.1731 Frame delay measurements

Management and Traffic Analysis

- RFC 2030 SNTP, Simple Network Time Protocol v4
- RFC 854 Telnet client and server
- RFC 783 TFTP Protocol (revision 2)
- RFC 951, 1542 BootP
- RFC 2131 BOOTP/DHCP relay agent and DHCP server
- RFC 1591 DNS (client operation)
- RFC 1155 Structure of Mgmt Information (SMIv1)
- RFC 1157 SNMPv1
- RFC 1212, RFC 1213, RFC 1215 MIB-II, Ethernet-Like MIB & TRAPs
- RFC 1573 Evolution of Interface
- RFC 1650 Ethernet-Like MIB (update of RFC 1213 for SNMPv2)
- RFC 1901, 1905 – 1908 SNMP v2c, SMIv2 and Revised MIB-II
- RFC 2576 Coexistence between SNMP Version 1, Version 2 and Version 3
- RFC 2578 – 2580 SMIv2 (update to RFC 1902 – 1903)
- RFC 3410 – 3415 SNMPv3, user based security, encryption and authentication
- RFC 3826 – The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
- RFC 1757 RMON 4 groups: Stats, History, Alarms and Events
- RFC 2021 RMON2 (probe configuration)
- RFC 2613 SMON MIB
- RFC 2925 Ping/Traceroute MIB
- RFC 2668 802.3 MAU MIB
- draft-ietf-hubmib-mau-mib-v3-02.txt
- RFC 1643 Ethernet MIB
- RFC 1493 Bridge MIB
- RFC 2096 IPv4 Forwarding Table MIB
- RFC 2737 Entity MIB v2
- RFC 2233 Interface MIB
- RFC 3621 PoE-MIB (PoE switches only)
- IEEE 802.1ag MIB
- Secure Shell (SSH-2) client and server
- Secure Copy (SCP-2) client and server
- Secure FTP (SFTP) server
- sFlow version 5
- Configuration logging
- Multiple Images, Multiple Configs
- RFC 3164 BSD Syslog Protocol with Multiple Syslog Servers
  - 999 Local Messages (criticals stored across reboots)
- Extreme Networks vendor MIBs (includes FDB, PoE, CPU, Memory MIBs)
- XML APIs over Telnet/SSH and HTTP/HTTPS
- Web-based device management interface – ExtremeXOS ScreenPlay™
- IP Route Compression
- Stacking – SummitStack™ (Summit products with Advanced Edge License and above only)

Security, Switch and Network Protection

- Secure Shell (SSH-2), Secure Copy (SCP-2) and SFTP client/server with encryption/authentication (requires export controlled encryption module)
- SNMPv3 user based security, with encryption/authentication (see above)
- RFC 1492 TACACS+
- RFC 2138 RADIUS Authentication
- RFC 2139 RADIUS Accounting
- RFC 3579 RADIUS EAP support for 802.1x
- RADIUS Per-command Authentication
- Access Profiles on All Routing Protocols
- Access Policies for Telnet/SSH-2/SCP-2
- Network Login – 802.1x, Web and MAC-based mechanisms
- IEEE 802.1x – 2001 Port-Based Network Access Control for Network Login
- Multiple supplicants with multiple VLANs for Network Login (all modes)
- Fallback to local authentication database (MAC and Web-based methods)
- Guest VLAN for 802.1x
- RFC 1866 HTML – used for Web-based Network Login and ExtremeXOS ScreenPlay
- SSL/TLS transport – used for Web-based Network Login and ExtremeXOS ScreenPlay (requires export controlled encryption module)
- MAC Security – Lockdown and Limit
- IP Security – RFC 3046 DHCP Option 82 with port and VLAN ID
- IP Security – Trusted DHCP Server
- Layer 2/3/4 Access Control Lists (ACLs)
- RFC 2267 Network Ingress Filtering
- RPF (Unicast Reverse Path Forwarding) Control via ACLs
- Wire-speed ACLs
- Rate Limiting/Shaping by ACLs
- IP Broadcast Forwarding Control
- ICMP and IP-Option Response Control
- SYN attack protection
- CPU DoS Protection with traffic rate-limiting to management CPU
- Robust against common Network Attacks:
  - CERT (http://www.cert.org)
  - CA-2003-04: “SQL Slammer”
  - CA-2002-36: “SSHredder”
  - CA-2002-03: SNMP vulnerabilities
  - CA-98-13: tcp-denial-of-service
  - CA-98.01: smurf
  - CA-97.28:Teardrop_Land -Teardrop and “LAND“ attack
  - CA-96.26: ping
  - CA-96.21: tcp_syn_flooding
  - CA-96.01: UDP_service_denial
  - CA-95.01: IP_Spoofing_Attacks_and_Hijacked_ Terminal_Connections
  - IP Options Attack
- Host Attacks
  - Teardrop, boink, opentear, jolt2, newtear, nestea, syndrop, smurf, fraggle, papasmurf, synk4, raped, winfreeze, ping –f, ping of death, pepsi5, Latierra, Winnuke, Simping, Sping, Ascend, Stream, Land, Octopus

Security, Router Protection

Requires Edge License or above

- IP Security – DHCP enforcement via Disable ARP Learning
- IP Security – Gratuitous ARP Protection
- IP Security – DHCP Secured ARP/ARP Validation
- Routing protocol MD5 authentication

Security Detection and Protection

In Core and Aggregation Products only

- CLEAR-Flow, threshold-based alerts and actions

IPv4 Host Requirements

- RFC 1122 Host Requirements
- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 894 IP over Ethernet
- RFC 1027 Proxy ARP
- RFC 2068 HTTP server
- IGMP v1/v2/v3 Snooping with Configurable Router Registration Forwarding
- IGMP Filters
- PIM Snooping
- Static IGMP Membership
- Multicast VLAN Registration (MVR)

IPv4 Router Requirements

Requires Advanced Edge License or above

- RFC 1812 Requirements for IP Version 4 Routers
- RFC 1519 CIDR
- RFC 1256 IPv4 ICMP Router Discovery (IRDP)
- Static Unicast Routes
- Static Multicast Routes
- RFC 1058 RIP v1
- RFC 2453 RIP v2
- Static ECMP
- RFC 1112 IGMP v1
- RFC 2236 IGMP v2

© 2010 Extreme Networks, Inc. All rights reserved.

Technical Specifications

IPv4 Router Requirements continued

Requires Advanced Edge License or above

- RFC 3376 IGMP v3
- RFC 2933 IGMP MIB
- RFC 2096 IPv4 Forwarding Table MIB
- RFC 1724 RIPv2 MIB
- RFC 3768 VRRPv2
- RFC 2787 VRRP MIB
- RFC 2328 OSPF v2 (Edge-mode)
- OSPF ECMP
- OSPF MD5 Authentication
- RFC 1587 OSPF NSSA Option
- RFC 1765 OSPF Database Overflow
- RFC 2370 OSPF Opaque LSA Option
- RFC 3623 OSPF Graceful Restart
- RFC 1850 OSPFv2 MIB
- RFC 2362 PIM-SM (Edge-mode)
- RFC 2934 PIM MIB
- RFC 3569, draft-ietf-ssm-arch-06.txt PIM-SSM PIM Source Specific Multicast
- draft-ietf-pim-mib-v2-o1.txt
- Mtrace, a "traceroute" facility for IP Multicast: draft-ietf-idmr-traceroute-ipm-07
- Mrinfo, the multicast router information tool based on Appendix-B of draft-ietf-idmr-dvmrp-v3-11

IPv6 Host Requirements

Current support on ExtremeXOS based Summit series, BlackDiamond 8800 series, BlackDiamond 10808 series and BlackDiamond 12800 series

- RFC 5095, Internet Protocol, Version 6 (IPv6) Specification
- RFC 4861, Neighbor Discovery for IP Version 6, (IPv6)
- RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification
- RFC 2464, Transmission of IPv6 Packets over Ethernet Networks
- RFC 2465, IPv6 MIB, General Group and Textual Conventions
- RFC 2466, MIB for ICMPv6
- RFC 2462, IPv6 Stateless Address Auto configuration – Host Requirements
- RFC 1981, Path MTU Discovery for IPv6, August 1996 – Host requirements
- RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture
- RFC 3587, Global Unicast Address Format
- Telnet server over IPv6 transport
- SSH-2 server over IPv6 transport
- Ping over IPv6 transport
- Traceroute over IPv6 transport

IPv6 Interworking and Migration

Current support on ExtremeXOS based Summit series, BlackDiamond 8800 series, BlackDiamond 10808 series and BlackDiamond 12800 series

- RFC 2893, Configured Tunnels
- RFC 3056, 6to4

IPv6 Router Requirements

Current support on ExtremeXOS based Summit series, BlackDiamond 8800 series, BlackDiamond 10808 series and BlackDiamond 12800 series

- RFC 2462, IPv6 Stateless Address Auto configuration – Router Requirements
- RFC 1981, Path MTU Discovery for IPv6, August 1996 – Router requirements
- RFC 2710, IPv6 Multicast Listener Discovery v1 (MLDv1) Protocol
- RFC 3810, IPv6 Multicast Listener Discovery v2 (MLDv2) Protocol
- Static Unicast routes for IPv6
- RFC 2080, RIPng
- Static ECMP

Core Protocols for Layer 2, IPv4 and IPv6

Requires Core License or above

- EAPSv2 Shared Ports – multiple interconnections between rings
- PIM-DM Draft IETF PIM Dense Mode draft-ietf-idmr-pim-dm-05.txt, draft-ietf-pim-dm-new-v2-04.txt
- RFC 3618 Multicast Source Discovery Protocol (MSDP)
- RFC 3446 Anycast RP using PIM and MSDP
- RFC 2740 OSPFv3, OSPF for IPv6 – *Current support on Summit series with Core License or above, BlackDiamond 8800 series, BlackDiamond 10808 series, and BlackDiamond 12800 series*
- RFC 1771 Border Gateway Protocol 4
- RFC 1965 Autonomous System Confederations for BGP
- RFC 2796 BGP Route Reflection (supersedes RFC 1966)
- RFC 1997 BGP Communities Attribute
- RFC 1745 BGP4/IDRP for IP-OSPF Interaction
- RFC 2385 TCP MD5 Authentication for BGPv4
- RFC 2439 BGP Route Flap Damping
- RFC 2918 Route Refresh Capability for BGP-4
- RFC 3392 Capabilities Advertisement with BGP-4
- RFC 4360 BGP Extended Communities Attribute
- RFC 4486 Subcodes for BGP Cease Notification message
- draft-ietf-idr-restart-10.txt Graceful Restart Mechanism for BGP
- RFC 4760 Multiprotocol extensions for BGP-4
- RFC 1657 BGP-4 MIB
- Draft-ietf-idr-bgp4-mibv2-02.txt – Enhanced BGP-4 MIB
- RFC 1195 Use of OSI IS-IS for Routing in TCP/IP and Dual Environments (TCP/IP transport only)
- RFC 2763 Dynamic Hostname Exchange Mechanism for IS-IS
- RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS
- RFC 2973 IS-IS Mesh Groups
- RFC 3373 Three-way Handshake for IS-IS Point-to-Point Adjacencies
- RFC 3784 IS-IS Externs for Traffic Engineering (wide metrics only)
- Draft-ietf-isis-restart-02 Restart Signaling for IS-IS
- Draft-ietf-isis-ipv6-06 Routing IPv6 with IS-IS – *Current support on Summit series with Core License or above, BlackDiamond 8800 series, BlackDiamond 10808 series, and BlackDiamond 12800 series*
- Draft-ietf-isis-wg-multi-topology-11 Multi Topology (MT) Routing in IS-IS

QoS and VLAN Services

Quality of Service and Policies

- IEEE 802.1D – 1998 (802.1p) Packet Priority
- RFC 2474 DiffServ Precedence, including 8 queues/port
- RFC 2598 DiffServ Expedited Forwarding (EF)
- RFC 2597 DiffServ Assured Forwarding (AF)
- RFC 2475 DiffServ Core and Edge Router Functions

VLAN Services: VLANs, vMANs

- IEEE 802.1Q VLAN Tagging
- IEEE 802.1v: VLAN classification by Protocol and Port
- Port-based VLANs
- Protocol-based VLANs
- MAC-based VLANs
- Multiple STP domains per VLAN
- Upstream Forwarding Only/Disable Flooding
- RFC 5517 Private VLANs
- VLAN Translation
- IEEE 802.1ad Provider Bridge Network, virtual MANs (vMANs)
- vMAN Ethertype Translation/Secondary vMAN Ethertype
- Multicast Support for PVLAN
- Multicast Support for VLAN Aggregation
- VLAN Aggregation (Requires Advanced Edge License or above)

Advanced VLAN Services

Requires Advanced Edge License or above (BlackDiamond 10808 and BlackDiamond 12800 series only)

- VLAN Translation in vMAN environments
- vMAN Translation

MAC-in-MAC (PBB)

Requires MPLS-PBB Feature Pack License

- IEEE 802.1ah/D1.2 Provider Backbone Bridges (PBB)/MAC-in-MAC

MPLS and VPN Services

Multi-Protocol Label Switching (MPLS)

Requires MPLS-PBB Feature Pack License or MPLS Feature Pack License

- RFC 2961 RSVP Refresh Overhead Reduction Extensions
- RFC 3031 Multiprotocol Label Switching Architecture
- RFC 3032 MPLS Label Stack Encoding
- RFC 3036 Label Distribution Protocol (LDP)
- RFC 3209 RSVP-TE: Extensions to RSVP for LSP Tunnels
- RFC 3630 Traffic Engineering Extensions to OSPFv2
- RFC 3811 Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management

© 2010 Extreme Networks, Inc. All rights reserved.

Technical Specifications

MPLS and VPN Services continued

Multi-Protocol Label Switching (MPLS)

Requires MPLS-PBB Feature Pack License or MPLS Feature Pack License

- RFC 3812 Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)
- RFC 3813 Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB)
- RFC 3815 Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)
- RFC 4090 Fast Re-route Extensions to RSVP-TE for LSP (Detour Paths)
- RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures (LSP Ping)

Layer 2 VPNs

Requires MPLS-PBB Feature Pack License or MPLS Feature Pack License

- RFC 4447 Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)
- RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks
- RFC 4762 Virtual Private LAN Services (VPLS) using Label Distribution Protocol (LDP) Signaling
- RFC 5085 Pseudowire Virtual Circuit Connectivity Verification (VCCV)
- draft-ietf-bfd-base-09.txt Bidirectional Forwarding Detection
- RFC 5542 Definitions of Textual Conventions for Pseudowire (PW) Management
- RFC 5601 Pseudowire (PW) Management Information Base (MIB)
- RFC 5602 Pseudowire (PW) over MPLS PSN Management Information Base (MIB)
- RFC 5603 Ethernet Pseudowire (PW) Management Information Base (MIB)
- draft-ietf-l2vpn-vpls-mib-02.txt Virtual Private LAN Services (VPLS) Management Information Base

www.extremenetworks.com

Corporate and North America
Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, CA 95051 USA
Phone +1 408 579 2800

Europe, Middle East, Africa and South America
Phone +31 30 800 5100

Asia Pacific
Phone +65 6836 5437

Japan
Phone +81 3 5842 4011

© 2010 Extreme Networks, Inc. All rights reserved. Extreme Networks, the Extreme Networks logo, BlackDiamond, EPICenter, Extreme Standby Router Protocol, ExtremeXOS ScreenPlay, Summit and SummitStack are either registered trademarks or trademarks of Extreme Networks, Inc. in the United States and/or other countries. sFlow is the property of Inmon Corporation. Specifications are subject to change without notice. 1030_09 06/10